ABSTRACT

[0085] An apparatus and method for unilaterally loading a secure operating system within a multiprocessor environment are described. The method includes disregarding a received load secure region instruction when a currently active load secure region operation is detected. Otherwise, a memory protection element is directed, in response to the received load secure region instruction, to form a secure memory environment. Once directed, unauthorized read/write access to one or more protected memory regions are prohibited. Finally, a cryptographic hash value of the one or more protected memory regions is stored within a digest information repository as a secure software identification value. Once stored, outside agents may request access to a digitally signed software identification value in order to establish security verification of secure software within the secure memory environment.